

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-208515

(43)Date of publication of application : 26.07.1994

(51)Int.Cl.

G06F 12/14

(21)Application number : 05-256786

(71)Applicant : BULL HN INF SYST INC

(22)Date of filing : 14.10.1993

(72)Inventor : HOLTEY THOMAS O
WILSON PETER J

(30)Priority

Priority number : 92 960748

Priority date : 14.10.1992

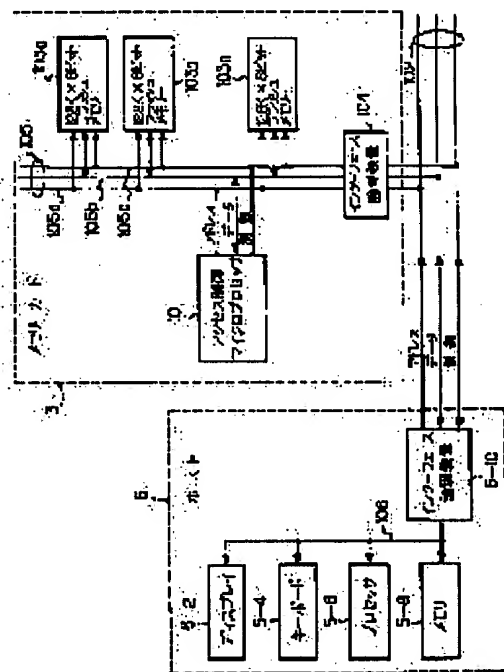
Priority country : US

(54) MEMORY CARD

(57)Abstract:

PURPOSE: To provide a security memory card containing a microprocessor on one semiconductor chip and one or more nonvolatile addressable memory chips.

CONSTITUTION: Both a microprocessor chip and a nonvolatile memory chip are connected to an internal card bus and addresses, data, and control information are transferred to the nonvolatile memory chip. A microprocessor 5-6 stores information containing many key values, configuration information peculiar to the use, and program instruction information. The memory of each chip is constituted in many blocks, namely, banks and each memory chip is constituted to contain a security control logic circuit. The circuits contain pluralities of nonvolatile and volatile storage devices which are loaded with keys and configuration information under the control of the microprocessor 5-6 only after the microprocessor 5-6 discriminates that a user successfully performs confirming procedures predecided by a host computer 5. Thereafter, the user is allow to read out information only from such a block as that defined by the configuration information.



LEGAL STATUS

[Date of request for examination]

29.06.1999

[Date of sending the examiner's decision of rejection]

08.04.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3493047

[Date of registration]

14.11.2003

[Number of appeal against examiner's decision of rejection] 2003-012861

[Date of requesting appeal against examiner's decision of rejection] 07.07.2003

[Date of extinction of right]

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-208515

(43)公開日 平成6年(1994)7月26日

(51)Int.Cl.⁵

G 0 6 F 12/14

識別記号

3 2 0 A 9293-5B

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数26 OL (全 19 頁)

(21)出願番号 特願平5-256786

(22)出願日 平成5年(1993)10月14日

(31)優先権主張番号 9 6 0 7 4 8

(32)優先日 1992年10月14日

(33)優先権主張国 米国(US)

(71)出願人 391031270

ブル・エイチエヌ・インフォメーション・
システムズ・インコーポレーテッド

BULL HN INFORMATION
SYSTEMS, INCORPORAT
ED

アメリカ合衆国マサチューセッツ州

01821, ビレリカ, テクノロジー・パーク

(番地なし)

(72)発明者 トーマス・オー・ホルティエ

アメリカ合衆国マサチューセッツ州02162,
ニュートン, クレホアー・ドライブ 10

(74)代理人 弁理士 湯浅 恭三 (外5名)

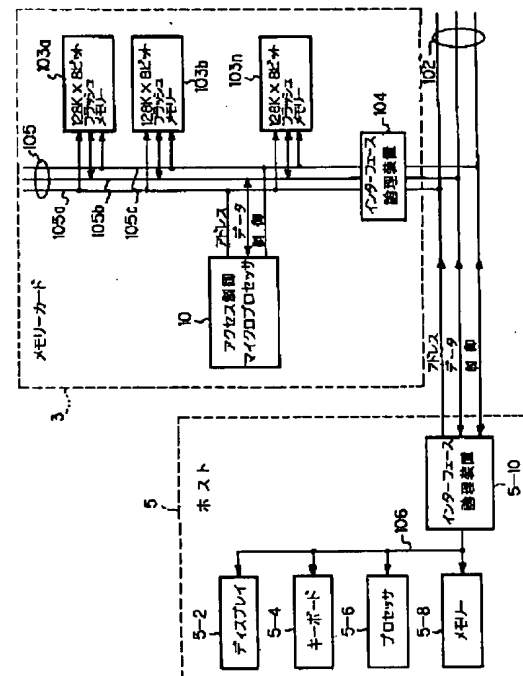
最終頁に続く

(54)【発明の名称】 メモリー・カード

(57)【要約】

【目的】1つの半導体チップ上のマイクロプロセッサと、1つ以上の不揮発性のアドレス指定可能なメモリー・チップとを含む機密保護メモリー・カードを提供する。

【構成】マイクロプロセッサ・チップと不揮発性メモリー・チップとは、共に内部カード・バスに接続して、アドレスとデータと制御情報とを前記不揮発性メモリー・チップへ転送する。マイクロプロセッサは、多数のキー値を含む情報と、用途に固有の構成情報と、プログラム命令情報とを含む。各チップのメモリーは、多数のブロック即ちバンクに構成され、各メモリー・チップは機密保護制御論理回路を含むように構成される。これらの回路は、ユーザがホスト・コンピュータによる予め定めた確認手順を成功裏に実施したことをマイクロプロセッサが判定した後にのみ、マイクロプロセッサの制御下でキーおよび構成情報でロードされる複数の不揮発性および揮発性の記憶装置を含んでいる。その後、ユーザは、構成情報により定義される如きブロックのみからの情報の読出しを許容される。



【特許請求の範囲】

【請求項1】 ホストの携帯コンピュータと共に使用される機密保護メモリ・カードにおいて、前記ホスト・コンピュータに対しおよびこれからアドレス、データおよび制御情報を送受するように接続されたマイクロプロセッサを設け、該マイクロプロセッサは、複数のキー値を含む情報と構成情報とを記憶するアドレス指定可能不揮発性メモリを含み、前記マイクロプロセッサに接続されて、アドレスとデータと前記カードにより行われるべきメモリ動作を定義する制御情報とを伝送する内部バスと、前記マイクロプロセッサと共通に前記内部バスに接続されて、前記アドレスとデータと制御情報とを受取る少なくとも一つの不揮発性のアドレス指定可能メモリとを設け、前記メモリは、不揮発性記憶セクションと機密保護制御セクションとを含み、該記憶セクションは複数のブロックに構成されたメモリ・アレイを含み、各ブロックは複数のアドレス指定可能な場所と前記記憶動作を行う制御論理手段とを有し、前記機密保護制御セクションは前記内部バスと前記制御論理手段と前記メモリ・アレイとに接続され、前記機密保護制御セクションは、前記ブロックと関連する少なくとも一つの前記キー値と構成情報を記憶する複数の不揮発性および揮発性記憶装置と、前記制御論理手段と前記記憶装置とに接続されたアクセス制御論理手段とを含み、該アクセス制御論理手段は、前記マイクロプロセッサが予め定めた確認手順が前記ホスト・コンピュータにより行われて前記アクセス制御論理手段が前記構成情報に従って前記メモリ・アレイからの前記情報の読出しを許容することを可能にしたと判定した後のみ、前記構成情報により指定される如き前記メモリ・アレイの前記ブロックのアドレス指定されたものに記憶された情報の読出しを可能にすることを特徴とするメモリ・カード。

【請求項2】 前記マイクロプロセッサおよび前記不揮発性メモリが個々の半導体チップ上に含まれることを特徴とする請求項1記載のメモリ・カード。

【請求項3】 前記カードが更に、該カードを前記ホスト・コンピュータに接続するインターフェース回路手段を含み、該インターフェース回路手段および前記マイクロプロセッサが同じ半導体チップ上に含まれることを特徴とする請求項1記載のメモリ・カード。

【請求項4】 前記不揮発性メモリ・カードおよび前記不揮発性記憶装置がフラッシュ・メモリであることを特徴とする請求項1記載のメモリ・カード。

【請求項5】 前記不揮発性記憶装置の一方が、前記一つのキー値と対応するロック値を記憶するロック・メモリであり、前記不揮発性装置の第2のものが前記ロック・メモリに接続するロック記憶可能化要素であり、

前記ロック・メモリが最初に前記ロック値でロードされ、前記ロック記憶可能化要素が、前記マイクロプロセッサの制御下で前記ロック値の修正を禁止する状態へ切換えられることを特徴とする請求項1記載のメモリ・カード。

【請求項6】 前記ロック値の記憶および前記ロック記憶可能化要素の切換えが、前記メモリ・カードの初期の製造中に起生することを特徴とする請求項2記載のメモリ・カード。

【請求項7】 前記揮発性記憶装置の一方が、数において前記構成情報を記憶するための前記メモリ・アレイのブロック数と対応する複数の記憶域を持つアドレス指定可能なアクセス制御メモリであり、該アクセス制御メモリが前記内部バスと前記アクセス制御論理手段とに接続され、前記予め定めた確認手順が、前記アクセス制御論理手段による前記アクセス制御メモリの可能化を生じる前記ホスト・コンピュータにより最初に成功裏に行われたことを判定した後のみ、前記アクセス制御メモリが前記マイクロプロセッサの制御下でロードされることを特徴とする請求項5記載のメモリ・カード。

【請求項8】 前記ロック・メモリにロードされた前記ロック値が全て1であり、前記機密保護制御セクションが更に、前記ロック・メモリに接続された全て1の検出回路を含み、該検出回路が前記全て1のロック値に応答して、前記機密保護制御セクションを有効にバイパスする信号を生成して、前記不揮発性メモリがあたかも前記機密保護制御セクションが含まなかったかのよう動作することを可能にすることを特徴とする請求項7記載のメモリ・カード。

【請求項9】 前記予め定めた確認手順の実施が、前記メモリ・カードが前記ホスト・コンピュータと通信するように最初に接続される時に初めて起生することを特徴とする請求項7記載のメモリ・カード。

【請求項10】 前記アクセス制御メモリが、前記ロック・メモリから前記ロック値を受取るように接続されたロック・レジスタと、コンパレータ回路と、前記マイクロプロセッサにより前記キー・レジスタに送られるキー値を記憶するキー・レジスタと、予め定めた時間間隔を定義するカウントを記憶する遅延カウンタと、前記アクセス制御メモリと前記コンパレータと前記遅延カウンタとに接続されたゲート手段とを含み、前記コンパレータ回路が、前記ロックおよびキー・レジスタと前記ゲート手段とに接続され、該ゲート手段が前記遅延カウンタに接続されて、前記遅延カウンタが前記予め定めた時間間隔の終りを信号した時前記ロック・レジスタにロードされる前記ロック・コード値間の同じ比較を信号する前記コンパレータ回路に回答してアクセス修正許容信号を生じ、前記アクセス修正許容信号が前記構成情報をロードするように前記アクセス制御メモリを条件付け

る信号を許容することを特徴とする請求項9記載のメモリー・カード。

【請求項11】 前記制御論理手段が、各メモリー・チップの前記機密保護制御セクションの動作を制御する際に前記マイクロプロセッサにより使用される予め定めた指令セットにตอบสนองして指令信号を生じる回路を含むことを特徴とする請求項10記載のメモリー・カード。

【請求項12】 前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの最初のものにตอบสนองして、前記ロック・コード値を前記ロック・メモリーにロードする第1の信号を生じ、該予め定めた指令の前記最初の前記カードの初期の製造中に生成されることを特徴とする請求項11記載のメモリー・カード。

【請求項13】 前記制御論理手段が、前記マイクロプロセッサにより生成された前記予め定めた指令セットの第2のものにตอบสนองして、前記ロック記憶可能化要素を、前記ロック・メモリーに記憶された前記ロック値に対する前記読出しまたは修正を禁止する予め定めた状態へ切換えるための第2の信号を生じることを特徴とする請求項12記載のメモリー・カード。

【請求項14】 前記制御論理手段が、前記マイクロプロセッサにより生じた前記予め定めた指令セットの第3のものにตอบสนองして、前記キー値の予め定めたもので前記予め定めたキー・レジスタをロードする第3の信号を生じ、前記予め定めた指令セットの前記第3のものが、前記予め定めた確認手順が成功裏に行われたことを前記マイクロプロセッサが判定した後にのみ、前記マイクロプロセッサにより生じることを特徴とする請求項12記載のメモリー・カード。

【請求項15】 前記制御論理手段により生じる前記第3の信号が、前記遅延カウンタを前記予め定めた時間間隔の開始を確立する予め定めたカウントに同時に強制し、前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの第4のものの各々にตอบสนองして前記予め定めたカウントを1だけ減分し、前記遅延カウンタが、前記予め定めた指令セットの予め定めた数の前記第4のものの実行に続く前記時間間隔の前記終りを信号することを特徴とする請求項14記載のメモリー・カード。

【請求項16】 前記予め定めた制御論理手段が、前記マイクロプロセッサによる前記予め定めた指令セットの第5および第6の複数にตอบสนองして、情報の読出しが許容される前記ブロックのどれかを判定するため前記構成情報に従って前記アクセス制御メモリーにおける場所をセットしリセットするための第5および第6の信号を生じることを特徴とする請求項11記載のメモリー・カード。

【請求項17】 前記ホスト・コンピュータとの通信を確立するためホストの携帯コンピュータに組み込み可能な

機密保護メモリー・カードにおいて、

単一の半導体チップ上に含まれるマイクロプロセッサを設け、該マイクロプロセッサは、前記ホスト・コンピュータに対しかつこれからアドレスとデータと制御情報とを送受するよう接続され、該マイクロプロセッサは、記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するメモリー読出しアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、

アドレスとデータと前記カードにより行われるべき記憶動作を定義する制御情報とを伝送する内部バスと、前記アドレスとデータと制御情報とを受取るため前記マイクロプロセッサと共通に前記内部バスに接続された少なくとも1つの不揮発性のアドレス指定可能なメモリー・チップとを設け、該メモリー・チップは1つの記憶セクションと1つの機密保護セクションとを含み、該記憶セクションはデータ出力を有する不揮発性のメモリー・アレイを含んで各々が複数のアドレス指定可能な場所を有する複数のブロックに構成され、前記記憶動作を行うための制御論理手段を含み、前記機密保護セクションは、前記内部バスと前記制御論理手段と前記データ出力とに接続され、該機密保護セクションは、

前記内部バスに接続されて前記キー値数の1つと合致する予め定めたロック値を最初に受取りかつこれを恒久的に記憶する不揮発性ロック・メモリーと、前記制御論理手段および前記ロック・メモリーと接続されて、前記予め定めたロック・コード値が前記マイクロプロセッサにより前記内部バスに与えられた前記キー値の選択された1つに識別可能に合致する時を検出すると同時に、可能化信号を生じるアクセス制御論理手段と、前記読出し可能性を定義する前記記憶構成情報を記憶するための数において前記メモリー・アレイの前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、前記アクセス制御メモリーが、前記制御論理手段と前記メモリー・アレイのデータ出力と前記内部バスと前記アクセス制御論理手段とに接続され、該アクセス制御論理手段は、予め定めた確認手順が前記ホスト・コンピュータにより成功裏に行われ、かつ前記記憶のキー・コードの前記予め定めた1つを転送して、前記アクセス制御メモリーの構成情報により指定される如き前記データ出力に加えるための前記可能化信号を、前記アクセス制御論理手段をして前記データ出力に加えられる前記可能化信号を生じさせたことを前記マイクロプロセッサが判定した後にのみ、前記記憶構成情報により指定される如き前記メモリー・アレイの読出しを可能にすることを特徴とするメモリー・カード。

【請求項18】 各々が複数のモードにおける動作能力を有するアドレス指定可能な場所のブロックに構成され

たメモリー・アレイを含む複数の不揮発性メモリー・チップを含む機密保護メモリー・カードにおいて、ロック値を記憶するロック・メモリーと、第1および第2の指令と予め定めたキー値とを生成する制御手段と、

前記制御手段に接続されて、前記第1の指令に回答して前記予め定めたキー値を記憶するキー・レジスタと、前記ロック・メモリーおよび前記キー・レジスタに接続され、前記ロック値および前記予め定めたキー値が等しい時は常に比較信号を生成するコンパレータと、前記生成手段に接続され、かつ前記第1の指令に回答して前記カウンタを最大カウント値に設定し、かつ一連の連続する第2の指令に回答して前記遅延カウンタがゼロに減分された時ゼロ・カウント信号を生じる遅延カウンタと、前記コンパレータおよび前記遅延カウンタに接続され、前記比較信号および前記ゼロ・カウント信号に回答してアクセス修正許可信号を生じる論理回路手段とを設け、前記制御手段が、第3の指令と、前記第1のブロックおよび以降のブロックをそれぞれ識別する第1のアドレス信号と以降のアドレス信号とを生じ、前記論理手段と前記制御手段とに接続されたアクセス制御メモリー手段を設け、該アクセス制御メモリーは、前記アクセス記憶可能化信号と前記アドレス信号と前記第3の指令とに回答して、前記ブロックおよび前記以降のブロックの内の一つが読出しのため可能状態にされる時を指定する表示を記憶することを特徴とするメモリー・カード。

【請求項19】 前記メモリー・カードが不当なホスト・コンピュータに配置される時、前記予め定めた値および最大値が、前記不揮発性メモリーに記憶された前記情報に対する容易なアクセスを阻止するように十分に大きく選定されることを特徴とする請求項18記載のシステム。

【請求項20】 前記制御手段が、第1のユーザの確認動作を成功裏に行ったと同時に、前記第1、第2および第3の指令を生じる前記メモリーに接続するマイクロプロセッサを含むことを特徴とする請求項18記載のカード。

【請求項21】 前記第1の指令がロード・キー指令であり、前記第2の指令が減分指令であり、前記第3の指令が読出し許可ブロック指令であることを特徴とする請求項20記載のカード。

【請求項22】 前記メモリーが更に、前記カードを正常な記憶動作を行うように条件付ける予め定めた指令セットを復号する指令制御手段を含み、前記指令制御手段が、前記第1、第2および第3の指令を含む別の指令セットを復号して前記メモリーに記憶された情報に対する機密保護を行う手段を含むことを特徴とする請求項18記載のカード。

【請求項23】 各々がアドレス指定可能な場所に構成されたメモリー・アレイを含む複数の不揮発性メモリー・チップと、記憶動作を行う指令信号を生じる制御論理回路を含むホスト・コンピュータに組み込み可能な機密保護メモリー・カードを構成する方法において、

(a) 組み込まれた時前記ホスト・コンピュータと通信するように接続される前記カードにマイクロプロセッサを組み込み、該マイクロプロセッサは、記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、

(b) 機密保護論理回路を各不揮発性メモリー・チップに組み込み、該機密保護論理回路が、予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メモリーと接続されたアクセス制御論理手段と、前記構成情報に従ってアクセス可能性のビット情報を記憶する前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、

(c) 前記マイクロプロセッサを各メモリー・チップに組み込み、アドレスとデータと制御情報とを前記各メモリー・チップへ転送し、

(d) 複数の指令に回答して前記機密保護論理回路を動作させるよう前記制御論理回路を修正し、

(e) 前記ホスト・コンピュータと共に前記マイクロプロセッサによる初期の予め確立されたユーザ確認動作を実施し、

(f) ステップ(e)における前記確認動作が成功裏に行われた時にのみ、前記各チップに対して前記複数の指令の特定のものを転送する前記マイクロプロセッサにより前記機密保護論理回路を可能状態にして、前記ブロックの異なるものに記憶された前記情報を前記アクセス制御メモリーに記憶された前記アクセス可能性ビット情報に従って読出すことを許可するステップを含むことを特徴とする方法。

【請求項24】 前記マイクロプロセッサの不揮発性メモリーが複数のセクションを有し、ステップ(a)が更に、前記キー値に対する乱数を生成して該キー値を前記セクション数の最初のものにロードするステップを含むことを特徴とする請求項23記載の方法。

【請求項25】 前記マイクロプロセッサが更に、前記マイクロプロセッサの不揮発性メモリーに接続されたインターバル・カウンタを含み、ステップ(a)が更に、ユーザが選択した時間間隔を生成して該ユーザ選択時間間隔値と対応する値を前記インターバル・カウンタへロードするステップを含み、更に

(g) 前記ユーザ選択時間間隔でステップ(e)の前記ユーザ確認動作を周期的に開始し、

(h) ステップ(b)の前記確認動作が成功裏に行われる限り、前記ブロックに記憶された前記情報が前記アク

セス可能性ビット情報に従って読出されることを許容し続けるステップを含むことを特徴とする請求項24記載の方法。

【請求項26】 各々がアドレス指定可能な場所のブロックに構成されたメモリー・アレイを含む多数の情報を記憶するための複数の不揮発性メモリー・チップと、記憶動作を行うための指令信号を生成する制御論理回路とを含む機密保護メモリー・カードを構成する方法において、

(a) 記憶域に対するユーザのアクセス可能性を定義する多数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含むマイクロプロセッサを前記カードに組み込み、

(b) 予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メモリーに接続されたアクセス制御論理手段と、前記構成情報に従ってユーザのアクセス可能性ビット情報を記憶する前記多数のブロックと数において対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含む機密保護論理回路を各不揮発性メモリー・チップに組み込み、

(c) アドレスとデータと制御情報とを前記各メモリー・チップへ転送するため前記マイクロプロセッサを各メモリー・チップに相互に接続し、

(d) 前記制御論理回路により通常与えられる1組の指令に対する拡張として前記機密保護論理回路を動作させる複数の指令を組み込むように前記制御論理回路を修正することにより、前記機密保護論理回路が、前記多数のチップが前記メモリー・カードから取外される場合でも、前記チップに含まれる前記情報が不当な方法で読出されることを防護するステップを含むことを特徴とする方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、携帯用パーソナル・コンピュータの分野に関し、特に可搬性デジタル情報環境におけるデータ機密保護のための保守システムに関する。

【0002】

【従来の技術】個人情報の機密保護はいつまでも問題である。この個人情報は、ロック、コードおよびシークレット・ポケットにより保証されてきた。情報が新しい形態をとると、変化した状況に見合うように新しい方法が要求されてきた。

【0003】歴史的には、情報の機密保護は、署名、印章および写真の使用により対処されてきた。自動銀行業務機械の如き電子装置は、コード化カードおよび個人の識別番号(PIN)を機密保護ツールのレパートリに加えた。コンピュータ・システムは、パスワードを使用し続けている。

【0004】特に、「スマート・カード」が機密保護ツールとして使用されている。この「スマート・カード」は、書込み可能な不揮発性メモリーと、1枚のチップとして作られプラスチック製「クレジット・カード」に組み込まれた簡単な入出力インターフェースとを備えた小型マイクロコンピュータである。このカードは、特に設計された装置と接続することを可能にする外部パッドを有する。カードのマイクロコンピュータに保持されるプログラムは、この装置と対話して、その不揮発性メモリー・データをパスワードの交換を任意に含む必要のアルゴリズムに従って読出しあるいは修正することを可能にする。メモリー情報を保護しかつ状況に従って種々の許容を行う特殊な技法が実現されてきた。例えば、米国特許第4,382,279号「オンチップ修飾可能メモリーを備えた単一チップ・マイクロプロセッサ(Single Chip Microprocessor with on-Chip Modifiable Memory)」は、処理および制御装置と同じチップに含まれる不揮発性メモリーの自動プログラミングを可能にするアーキテクチャを開示している。他のシステムにおけるように、マイクロプロセッサは単に同じチップ上のメモリーを保護するに過ぎない。

【0005】「スマート・カード」は、識別のプロセスを容易にすると共に重要な情報を使えるようにするために用いられてきた。このような場合に、大半の過去の状況における如く、「キー」の物理的存在ならびにある特別な知識が、検証または確認プロセスの一部として用いられて来た。上記のこのような場合に、識別は、アクセスを要求する個人と機密保護ガードまたは自動出納機械の如き固定された機関との間の対話であった。

【0006】自立する計算装置の可搬性の今日の状態は、物理的なキーと確認機関の両者を小型で可搬性のあるものにし、従って更に紛失または盗難が避けられなくなる。更に、計算装置は、識別プロセスと関連する特殊な知識またはパスワードを考えあるいは推論する試みを何度も行うことを可能にする。これは、確認機関または装置もまた泥棒または強盗の手中にある場合にも特に妥当する。更に悪いことには、技術は今や災難から免れないポケットまたはハンドバッグに大量の敏感な情報を携行することを許しかつ促すものである。

【0007】今日では、ノートブックおよびサブノートブック・サイズのコンピュータが、著しい計算能力を許容しこのため更なるデータ格納容量の必要を生じる可搬性のある自立環境を提供する。このことは、最初はプログラムとデータの両方を保持する小型ハード・ディスク装置により遭遇した。パスワード保護は、これらのシステムにおいてしばしば用いられているが、第1に、確認機関自体が被害を受け易いため、敏感なデータを完全に保護するものではない。しかし、更に、データを保持するディスク・ドライブは、物理的に取外すことができ、

かつデータ分析を更に容易にする設定においてアクセスすることができる。この場合、ある形態の暗号化だけがデータの保護を可能にする。ディスク・アクセスの性質が、不当な行為もしくはコストの障壁なしにこれを可能にする。このような形式のシステムの一例は、米国特許第4,985,920号「集積回路カード(Integrated Circuit Card)」において記述されている。

【0008】フラッシュ・メモリーおよび取外し可能「記憶カード」の最近の出現により、携帯型コンピュータの寸法および給電要件の大きな低減を可能にした。このフラッシュ・メモリーは、ランダム・アクセス・メモリー(RAM)の柔軟性をディスクの性能に結付ける。今日では、これら技術の組み合わせにより、紙を必要とすることなく20,000,000バイトまでのデータをクレジット・カード・サイズの取外し可能パッケージに保有することを可能にする。このデータは、あたかも従来のディスク・ドライブに保持されるかのように、あるいはホストのメモリーの拡張であるかのようにホスト・システムから見えるようにすることができる。これらの技術の進展は、ハンドバッグまたはブリーフケースよりもポケットで携行される如き程度までシステム・サイズの更なる減少を可能にした。

【0009】このため、データおよびそのホスト・システムは、紛失または盗難を受け易くなると同時に、大きなコストおよび性能上の障壁となるため、暗号化によりメモリーのデータを保護することを更に困難にした。

【0010】

【発明が解決しようとする課題】従って、本発明の主たる目的は、機密保護メモリー・サブシステムを備えた携

【0011】本発明の別の目的は、携帯型デジタル・システムから取出されても保護することができるメモリー・カードの提供にある。

【0012】本発明の更に他の目的は、かかるカードのチップが取出されても保護されるメモリー・カードの提供にある。

【0013】

【課題を解決するための手段】上記の目的は、本発明の望ましい実施態様の機密保護カードにおいて達成される。この機密保護メモリー・カードは、単一の半導体チップ上のマイクロプロセッサと、1つ以上の不揮発性のアドレス指定可能なメモリー・チップとを含んでいる。このマイクロプロセッサ・チップおよび不揮発性メモリー・チップは、共にアドレス、データおよび制御情報をこのような不揮発性メモリー・チップへ送るための内部カード・バスに接続している。マイクロプロセッサは、内部バスにおけるアドレス、データおよび制御情報の転送を制御するための複数のキー値、構成情報およびプログラム命令情報を含む情報を記憶するためのアドレス指

定可能な不揮発性メモリーを含む。チップ・メモリーは、各々が複数のアドレス指定可能な記憶場所を有する複数のブロック即ちバンクに構成される。

【0014】本発明によれば、各メモリー・チップは、機密保護制御論理回路を含むように構成される。望ましい実施態様においては、これら回路は、マイクロプロセッサの制御下でロード可能な不揮発性ロック・メモリー、不揮発性ロック記憶可能化要素および揮発性アクセス制御メモリーを含む。更に、マイクロプロセッサは、第1に、ロック値を不揮発性ロック・メモリーにロードし、アクセスを禁止するロック記憶可能化要素をリセットする。その後、マイクロプロセッサは、構成情報により指定されるようにアクセス制御メモリーをロードする。このような情報は、ユーザがホスト・コンピュータによる予め定めた確認手順を成功裏に行ったことをマイクロプロセッサが判定した後のみロードされる。各メモリーの機密保護論理回路は、メモリー・チップのアクセス制御メモリーにロードされた構成情報の関数として、フラッシュ・メモリーの選択されたアドレス指定可能なブロックに記憶された情報の読出しを可能化する。周期的に、ユーザはホスト・コンピュータによる確認手順をうまくゆくように行うことが要求され、またユーザはアクセス制御メモリーにより許容される如き情報の読出しを継続することが許される。望ましい実施態様においては、ホスト・コンピュータは、パーソナル・コンピュータ・メモリー・カード国際協会(PCMCIA)規格と合致するインターフェースの如き標準的インターフェースを介してメモリー・カードに接続される。

【0015】本発明は、電子的な小型化が生成する「機密保護」環境におけるフラッシュ・メモリー技術により可能にされる大量のデータの保護を可能にするための要諦である「スマート・カード」と「メモリー・カード」技術を融合する。更に、本発明は、両技術における改善および強化を利用することができる。

【0016】更に、本発明の機密保護論理回路は、フラッシュ・メモリーの基本的論理回路に対して行うことが要求される変更量を最小化するように、フラッシュ・メモリーに組込まれてこれと関連して動作する。更に、フラッシュ・メモリーは、機密保護モード、および機密保護論理回路がバイパスされてフラッシュ・メモリーがこの回路が組込まれなかったかのように動作することを可能にする非機密保護モードで動作することができる。通常、非機密保護モードには、フラッシュ・メモリーの不揮発性ロック・メモリー内容がクリアされる時に入る。これは一般に、予め定めた状態(即ち、全て1の状態)に自然に消去するプログラムされないか完全に消去されたフラッシュ・メモリーを示す。

【0017】少量のロジックをフラッシュ・メモリーおよび「アクセス制御プロセッサ(ACP)」に加えることにより、フラッシュ・メモリーの内容はデータの暗号

化を必要とせずに機密保護される。従って、本発明は、大きなデータ・ブロックに対しては非常に時間を費やし得るデータの暗号化および解読のオーバーヘッドを排除する。

【0018】動作において、ACPは、システムのユーザにある形態の確認の入力を周期的に促す。これは、パスワード、PIN、特定のベン・コンピュータの筆記面上の特定点で行われる「ジェスチャ」、ユーザの音声による指令即ち「音声プリント」であり得る。方法はシステムによって異なる。プログラム可能ACPは、ユーザが確認の特定内容およびプロンプトの周期を変更することを許容する。ロックおよびアクセス制御メモリーにより要求される確認に対するコードおよびデータは、ACPと同じチップ上にあるACP不揮発性メモリー内に記憶され、従って保護される。

【0019】先に述べたように、良好な確認はACPをしてアクセスのためフラッシュ・メモリーの全てまたは選択されたブロックを可能状態にさせあるいは可能状態を継続させる。障害が、フラッシュ・メモリーに対するアクセスを不能にさせる。このため、この動作は、確認を良好に完了し損なうとフラッシュ・メモリーのデータを保護させることになる点において「デッドマン・スロットル」に類似している。更に、ユーザにより発された指令もまた、アクセスを不能にさせ得る。更に、給電オフ状態からの最初の給電と同時に、保護されたメモリー内容に対するアクセスは、最初の確認が成功裏に行われるまで阻止される。

【0020】このため、メモリー・カードまたはそのホスト・プロセッサのいずれか一方が失われるか、盗まれるか、消滅されるか、あるいは接続されないままにおかれるならば、メモリーのデータは、即時あるいはその時の周期的確認が終了直後のアクセスから保護される。盗難の場合は、メモリー・データは、メモリー・カードが開路されて電子的にプローブされるか、あるいはメモリー・チップが取外されて別の装置に置かれても、アクセスから保護される。

【0021】本発明の上記の目的および利点については、添付図面に関して以降の記述を読めば更によく理解されよう。

【0022】

【実施例】図1は、パーソナル・コンピュータあるいはトランザクション・プロセッサとして使用可能な携帯可能な機密保護コンピュータ・システム1のブロック図である。システム1は、バス102によりホスト・プロセッサ5と接続する本発明により構成されたメモリー・カード3を含む。ホスト・プロセッサ5は、Hewlett-Packard社製のHP95LXの如きバームトップ・パーソナル・コンピュータの形態をとり得る。ホスト・プロセッサ5は、全て共通にバス106と接続される液晶ディスプレイ(LCD)5-2と、キーボード

5-4と、マイクロプロセッサ5-6と、メモリー5-8と、直列インターフェース5-10を含む。メモリー5-8は、1Mバイトの読出し専用メモリー(ROM)と、512Kバイトのランダム・アクセス・メモリー(RAM)とを含む。

【0023】メモリー・カード3とホスト・プロセッサ5との間の接続は、標準的バス・インターフェースを介して確立される。望ましい実施態様においては、バス102は、パーソナル・コンピュータ・メモリー・カード国際協会(PCMCIA)規格に合致している。バス102は、ホスト・プロセッサ5とメモリー・カード3間に標準的インターフェース・チップ104およびメモリー・カード・バス105を介してアドレス、制御およびデータ情報を送るための経路を提供する。バス102、105、106の各々は、データ・バス、制御バスおよびアドレス・バスを含み、全ての類似のバスを介する連続的な信号経路を提供する。例えば、バス105は、アドレス・バス105aと、データ・バス105bと、制御バス105cとを含む。

【0024】PCMCIAバス規格は、メモリー・カード上のディスク・エミュレーションをサポートする規格からメモリー・データに対するランダム・アクセスを可能にする実質的に異なる規格へ展開した。本発明のメモリー・カードは、暗号化技術によらずにランダムな記憶場所に対する迅速なアクセスを行うことにより、この新しい規格をサポートする保護技術を提供する。メモリー・アレイからホストへデータを運ぶデータ経路を制御することにより、本発明のメモリー・カードは、時間を費やすバッファリング、暗号化あるいはこの経路における他の逐次処理を用いることなくデータを保護する。

【0025】典型的には、ユーザは、キーボード5-4からシステム1を操作して、ディスプレイ5-2上に情報を表示してメモリー・カード3にファイル単位で記憶された情報を更新する表計算およびデータベース機能の如き典型的な動作を行う。ホスト・プロセッサ5は、アドレス情報をバス102に送出して情報を検索し、必要に応じて、この情報を更新してこれを必要なアドレスおよび制御情報とともにメモリー・カード3へ返送する。

【0026】図1に示されるように、本発明のメモリー・カード3は、バス105と接続されたアクセス制御プロセッサ(ACP)10と、各々バス105と接続された複数(n個の)のCMOSフラッシュ・メモリー・チップ103a乃至103nとを含む。ACP10は、典型的には「スマート・カード」において使用されるものと同じ形式の処理要素である。CMOSフラッシュ・メモリー103a乃至103nは、Intel社製のフラッシュ・メモリー・チップの形態を呈するものでよい。例えば、これらは、8個の128Kバイト×8個のCMOSフラッシュ・メモリーを含むIntel 28F001BX 1Mと呼ばれるIntelフラッシュ・メモ

リー・チップの形態のものでよい。このため、4Mバイトのフラッシュ・メモリー・カードは、32個のCMOSフラッシュ・メモリーを含む、即ち、「n」=32。

【0027】(アクセス制御プロセッサ10)図2は、望ましい実施態様のアクセス制御プロセッサ(ACP)10をブロック図の形態で示している。図示の如く、ACP10は、バス105と接続された保護不揮発性メモリー10-2と、ランダム・アクセス・メモリー(RAM)10-4と、マイクロプロセッサ10-6と、インターバル・カウンタ10-8と、インターフェース・ブロック10-10とを含む。不揮発性メモリー10-2は、確認情報およびプログラムを記憶する複数のアドレス指定された記憶場所を専用化する。更に、記憶域10-2aは、1つ以上の個人の識別番号(PIN)、プロトコル・シーケンス、あるいはユーザがシステムに対してアクセスしたことを識別しかつ再確認のため使用される時間間隔値に加えてユーザがアクセスし得るフラッシュ・メモリー103a乃至103nにおけるブロックを識別するための他の識別情報を記憶する。

【0028】記憶域10-2bは、フラッシュ・メモリー103a乃至103nの各々の保護のため使用されるキー値またはフラッシュ・メモリー103a乃至103nの各々のこのブロックを保護するため使用されるコードを記憶する。

【0029】記憶域10-2cは、要求される確認操作を実行するため、また障害に対して予め設定された条件が満たされるならば、システムをクリアするためのプログラム命令シーケンスを記憶する。あるプログラム命令は、ユーザの再確認が生じる時を確立するインターバル・カウンタ10-8のセッティングをユーザが制御することを可能にする。この再確認間隔は、割込みと、ユーザにPINまたは他のパスワードを再び入れさせることによりユーザの同一性の検証を要求するホスト・プロセッサ5に対する割込みとの間の時間を定義する。インターバル・カウンタ10-8は、バス102によりホスト・プロセッサ5からのクロック・パルスを受取り、作業環境に従ってユーザにより設定することができる。例えば、家庭において、ユーザはタイマーをオフにする(即ち、タイマーを最大値に設定する)か、あるいはタイマー間隔を1時間に設定することもできる。航空機において、保護を増すためにユーザはこのタイマーを10分に設定することもできる。先に述べたように、ユーザは、「パワーオン」毎にこの間隔のセッティングを再検査するように促され、これにより周期的な再確認を強制して機密保護を実施する。

【0030】(フラッシュ・メモリー103a乃至103n)図3は、フラッシュ・メモリー103a乃至103nの詳細なブロック図である。メモリー103b乃至103nはメモリー103aと同一に構成されているため、メモリー103aの詳細な論理回路のみが示され

る。

【0031】フラッシュ・メモリー103aは、基本的には2つのセクション、即ち、本発明の機密保護アクセス制御回路を含む1つのセクションと、フラッシュ・メモリーの基本的即ち標準的な論理回路を含む別のセクションとからなる。

【0032】(機密保護アクセス制御セクション)図3から判るように、本発明の機密保護制御回路は、図示の如く配置された32ビットのキー・レジスタと、32ビット揮発性ロック・レジスタ33と、12ビット遅延カウンタ32と、コンパレータ回路39と、全て1検出信号回路38と、不揮発性ロック・メモリー35と、1ビット不揮発性ロック記憶可能化要素36と、揮発性アクセス制御メモリー43と、アクセス修正許容ANDゲート34と、出力ORゲート45とを含む。このセクションは、基本的論理セクションに含まれる指令レジスタ50からの種々の16進数値(例えば、31H乃至38H)により示される指令制御信号を受取ること注目されたい。これらの信号は、ACP10からデータ・バス105bを介して指令レジスタ50により受取られる指令セットの異なるデータ値を表示する。これらの指令は、通常フラッシュ・メモリーにより使用される指令セットに対する重要な拡張である。標準的フラッシュ・メモリー指令は、28F001BXフラッシュ・メモリーにより用いられる指令の形態をとる。これら指令については、参考のため本文に援用されるIntel社の「メモリー製品(Memory Products)」に記載されている。本発明により使用される指令は、表1に記載されている。

【0033】表1に示される最初の指令は、乱数生成ロック値をメモリー103a乃至103nの各々における不揮発性ロック・メモリー(LM)35へ最初にロードするため使用されるロード・ロック・メモリー指令である。メモリー103a乃至103nの各々は、ユーザの機密保護の必要に従って異なるロック値または同じロック値を有する。このロック値は、1ビット不揮発性ロック記憶要素36の制御下でキー(K)レジスタ31を介してLM35へロードされる。表1のリセット・ロック記憶可能化指令は、記憶要素36のリセットに用いられる。これは、リセット・ロック記憶可能化指令により一旦リセットされた記憶要素36はセットできないため、LM35に記憶されたロック値が変更されることを阻止する。LM35の不揮発性の内容は、パワーアップと同時にLレジスタ33へ送られる。ロック・メモリー35の場所即ちサイトが設計に依存することが判るであろう。例えば、メモリー35は、メモリー・アレイ54に対する拡張として構成することができる。

【0034】表1のロード・キー・レジスタ指令は、キー(K)レジスタ31をロードしかつ遅延カウンタ32をセットするために使用される。この減分遅延カウンタ

の指令は、遅延カウンタ32の内容を1だけ減分するためACP10により使用される。読出し許容メモリー・バンクおよび読出し不能化メモリー・バンク指令は、アクセス制御メモリー43のロード中メモリー・アレイ5*

*4の異なるメモリー・ブロックに対するアクセスを可能化あるいは不能化するためACP10により使用される。

【0035】

表 1

指 令	第1バス・ サイクル動作	アドレス日付	第2バス・サイクル 動作アドレス	日 付
ロック・ メモリー ロード	書込み	31H	書込み	N/A
ロック・ 記憶可能化 リセット	書込み	33H	N/A	N/A
キー・ レジスタ ロード	書込み	32H	書込み	キー日付
遅延カウ ンタ減分	書込み	35H	N/A	N/A
メモリー・ バンク読出 し許容	書込み	MBA 34H	書込み	MBA
メモリー・ バンク読出 し不能化	書込み	MBA 38H	書込み	MBA

ロック・メモリーをロード(31H)

この指令は、ロック記憶可能化要素36の出力信号が「真」である場合のみ、キー・レジスタ31の内容を不揮発性ロック・メモリー35へコピーする。

【0036】ロック記憶可能化をリセット(33H)

この指令は、ロック記憶可能化論理要素36をリセットして、これによりロック・メモリー35のロードまたは変更を禁止する。

【0037】キー・レジスタをロード(32H)

この指令は、キー・レジスタ31の前の内容を1バイト(LSBからMSBへ)だけシフトし、ACP10からの「キー値」をキー・レジスタのLSBにロードする。更に、この指令は遅延カウンタ32をその最大値、例えば全て「1」にセットする。

【0038】遅延カウンタを減分(35H)

この指令は、遅延カウンタ32を1だけ減分する。遅延カウンタは、メモリー・アレイ54の以降の読出しを許容するには「0」と等しくなければならない。

【0039】メモリー・バンクを読出し許容(34H)

この指令は、アクセス修正許容信号37が「真」であるならば、アクセス制御メモリー43におけるメモリー・バンク・アドレス(MBA)と対応するビットをセットする。これは、選択されたバンクへの読出しアクセスを許容する。

【0040】

メモリー・バンクを読出し不能化(38H)

この指令は、アクセス制御メモリー43におけるメモリー・バンク・アドレスと対応するビットをリセットする。

【0041】表1を更に詳細に考察すれば、表1が加えられた指令の各々に対するバス・サイクル動作をも示すことが判る。2バス・サイクルを要求する各指令に対して、最初のバス・サイクル毎に、指令レジスタ50がACP10により生じ、バス105のデータ・バス105aおよび入力バッファ51を介して送られた8ビット指令を受取る。指令レジスタ50は、2番目のバス・サイクルの間選択された論理要素がデータ・バス105bから指令を実行するため必要な情報を受取るよう条件付けする。明らかなように、リセット・ロック記憶可能化および減分遅延カウンタ指令が実行のために1サイクルのみを必要とするため、この2番目のバス・サイクルは、使用不能(N/A)と表示される。

【0042】正常動作中、Kレジスタ31は、ロード・キー・レジスタ指令により記憶場所10-2bから受取ったキー値でロードされ、遅延カウンタ32はその最大値にセットされる。遅延カウンタ32は、ACP10から受取る連続的な減分遅延カウンタ指令に回答して全て「ゼロ」に減分され、AND34に入力として与えられるゼロ・カウント出力信号41を生じる。

【0043】各遅延カウンタ32は、泥棒がチップを外してこれらを「違法カード」に取付けて各メモリー・チップのキーを推理するためプロセッサ即ち装置を反復的

に試行するようにプログラムする場合に、フラッシュ・メモリー103a乃至103nをアクセスするため行うことができる試行即ち試みの回数を制限する。換言すれば、カウンタ32は、フラッシュ・メモリーに対する不法なアクセスを獲得するために非常に多くの回数の試行即ち試みを行わねばならないことを保証する。キーおよび遅延カウンタのサイズは、このような試みが異常な時間を要することを必要とするように選択される。

【0044】更に、キー・レジスタ31は、略々四十億(2^{32})の異なる組合わせを記憶する。望ましい実施態様においては、遅延カウンタ32は12ビット・カウンタである。遅延カウンタ32がマイクロ秒毎に1回減分されるものとすれば、キー値の推論の試み毎に 2^{32} 即ち4ミリ秒を要することになる。正しいキー値を知るACP10は、最初のセットアップにおいて4ミリ秒の遅れを生じるに過ぎない。キー値を推理するランダムな試みは、50%の成功率を得るためには 2^{31} 回の試みを必要とする。これは、キー値を推理するために $2^{31} \times 2^{32}$ ミリ秒、即ち102日を要する。この時間は、大半の泥棒を諦めさせるに充分である。無論、キーおよび遅延カウンタ32のサイズを修正することにより、より長い短い時間を与えることも可能である。

【0045】本発明のメモリー・カードが盗まれて「不法なホスト」に取付けられる場合には、ACP10は、既知の手法でPINを推理する泥棒の試み回数を制限する。このような手法は、不当な推理の閾値を越えるならば、アクセスをロックするかあるいはデータを破壊することを含み得る。

【0046】フラッシュ・メモリー103aに対する最初の確認動作中、キー値は、4回連続するロード・キー・レジスタ指令に応答してキー値が32ビットのKレジスタ31へロードされる(即ち、データ・バス105bが1バイト幅のバスである)。遅延カウンタ32は、連続する最初のバス・サイクルにおいて減分遅延カウンタ指令を送るACP10により(全て「1」の)その最大カウントに強制されて減分される。遅延カウンタ32は「0」に減分されると、ANDゲート34の1つの入力に与えられるゼロ・カウント信号41を生成する。

【0047】Kレジスタ31に記憶されたキー値が対応するLレジスタ33に記憶されたロック値と等しくユーザが正しい識別をホスト・プロセッサ5へ与えたことを示すならば、比較ロジック39が等価比較信号42をANDゲート34の別の入力へ与える。これは、ANDゲート34をしてその出力にアクセス修正許容信号37を生じさせ、これがACP10の制御下でアクセス制御メモリー43に対する書込みを可能化する。これは更に、メモリー・アレイ54の読出しを後で許容する。

【0048】アクセス制御メモリー43は、メモリー・アレイ54の各ブロック/バンクに対して1ビットの揮発性記憶域を保持する。これらのビットは、フラッシュ

・メモリーのパワーアップ・シーケンスの一部として「ゼロ」にクリアされる。データがメモリー103aから読出されるためには、アドレス指定されたメモリー・ブロックと対応するビットが論理値「1」でなければならない。これらビットは、アクセス修正許容信号37が「真」である場合にのみACP10によりセットされて読出し許容修正許容信号37を生じる。

【0049】表1に示されるように、読出し許容メモリー・バンク指令の2番目のバス・サイクルの間、メモリー・アレイ54の選択されたメモリー・バンクの3つの上位アドレス・ビットがアドレス・バス105cに送出されると共に、16進数の指令識別子の反復がデータ・バス105aを介して指令レジスタ50へ送られる。その結果、「1」がアクセス制御メモリー43におけるアドレス指定されたビット場所へ書込まれることになる。望ましい実施態様においては、メモリー・アレイ54がそれぞれ16Kバイトの8つのバンクに構成されるため、読出し許容メモリー・バンク指令シーケンスが8回繰返される。ACP10は、類似の方法で読出し不能化メモリー・バンク指令のシーケンスを発することにより選択されたバンクに対するアクセスを制限することもできる。

【0050】本発明のアクセス制御メモリー43の出力は、メモリー・アレイ54のどれかのバンクの記憶域の内容が読出されつつある各フラッシュ・メモリー読出しサイクルの間、出力バッファ52に対して可能化入力として与えられる。即ち、1読出しサイクルが生じるが、適当なバンクのアクセス制御メモリーのゲート信号のない時は読出されたデータが出力バッファ52を通過することが禁止される。特に、望ましい実施態様の場合は、アクセス制御メモリー43は、8つの個々にアドレス指定可能なビット記憶要素と、各記憶要素の入力に接続された入力アドレス3乃至8ビット・デコーダと、各記憶要素の出力の接続された1乃至8出力マルチプレクサ回路を含む。各アドレスの3つの上位アドレス・ビットは、復号されてその内容が変更されるべきブロックに対する記憶要素を選択するため使用される。同様に、同じ3ビットが、読出されるフラッシュ・メモリーの記憶域を含むブロックに対する記憶要素の出力を選択するため使用される。

【0051】ロック・メモリー35が完全に消去される、即ち全て「1」のLレジスタ33の内容により示される如き全て「1」であるならば、出力バッファ52は常に可能状態になる。即ち、ロック・レジスタ33が「全て1」を含む時、これは「全て1」検出要素38からORゲート45に対する信号を生成して出力バッファ52を可能状態にする。これは、フラッシュ・メモリー103aを有効に非機密保護モードに置く。これは、本発明の全ての機密保護論理回路をバイパスさせる。従って、同じフラッシュ・メモリー・チップを機密保護およ

び非機密保護の両用途に使用することができ、これにより生産経済をもたらす結果となる。

【0052】（フラッシュ・メモリーの基本論理回路）図3および図4に示されるように、この回路は、メモリー・アレイ54と、指令レジスタ50と、入出力論理回路60と、アドレス・ラッチ56と、書込み状態マシン61と、消去電圧システム62と、出力マルチプレクサ53と、データ・レジスタ51と、出力バッファ52と、状態レジスタ58とを図のように含む。フラッシュ・メモリー103aの基本論理回路は先に述べたよう

＊のような回路は周知であるため、必要な程度に述べるに止める。この回路に関するこれ以上の情報については、文献「メモリー製品（Memory Products）」（注文番号210830、Intel社1992年発行）の3-109乃至3-134ページを参照されたい。図3および図4に示されるように、フラッシュ・メモリーの基本回路は、多数の入力信号（A0～A16）、アドレス、データ信号（D00～D07）および制御信号（CE、WE、OE、PWDおよびVPP）を受取る。これら信号については、表2において以降に記述する。

【0053】

表 2

記号

名前および機能

A0～A16 メモリー・アドレスに対する「アドレス入力」。アドレスは書込みサイクルの間内部的にラッチされる。

【0054】D00～D07 「データ入出力」：メモリー書込みサイクル間の入力データおよび指令はメモリーおよび状態読出しサイクルの間データを出力する。データ・ピンはハイのアクティブ状態にあり、チップが選択から外されるか出力が消勢される時、3状態のオフフロートする。データは書込みサイクルの間内部的にラッチされる。

【0055】CE チップ可能化：装置の制御ロジック、入力バッファ、デコーダおよび検出増幅器を付勢する。CEはローのアクティブ状態であり、CEハイが記憶装置の選択を外して、電力消費を待機レベルに低減する。

【0056】PWD パワーダウン：装置を深いパワーダウン・モードに置く。PWDがローのアクティブ状態にあり、PWDハイが正常な動作をゲートする。PWD=VHHは、メモリー・ブロックのプログラミングを可能にする。PWDはんだ、ローのアクティブ状態にある時消去または書込み動作をロックして、電力の供給中にデータ保護を行う。

【0057】OE 出力可能化：読出しサイクルの間装置の出力をデータ・バッファを通して装置の出力をゲートする。OEはローにアクティブ状態にある。

【0058】WE 書込み可能化：指令レジスタ置くアレイ・ブロックへの書込みを制御する。WEはローのアクティブ状態にある。アドレスおよびデータは、WEパルスの立上がりエッジと同時にラッチされる。

【0059】Vpp アレイの消去ブロックあるいは各ブロックのプログラミング・バイトに対する消去／プログラム給電。注：Vpp < Vpp1 Maxの時、メモリー内容は変更できない。

【0060】表2に示されるように、チップ可能化（CE）、書込み可能化プロセッサ（WE）および出力可能化（OE）の諸信号は、ホスト・プロセッサ5からバス102置く制御バス105bを介して指令レジスタ50

および入出力論理回路60へ与えられ、制御指定論理ブロックへ分散される。パワーダウン（PWD）信号もまた、フラッシュ・メモリーが表2で指定された諸動作を行うことを可能にするため指令レジスタ50へ与えられる。この信号は、必要に応じてフラッシュ・メモリーの機密保護制御セクションの揮発性記憶要素をクリヤするため使用することができ、これにより正常な動作が再び再開されると、ユーザの再確認を強化する。

【0061】一般に、フラッシュ・メモリーの基本論理要素は下記のように動作する。情報は、アドレス・バス105cからのアドレス・ロジック56により受取られるアドレスにより指定されるメモリー・ブロックの1つのアドレス指定された場所におけるデータ・バス105a、入力バッファ51およびデータ・レジスタ55を介してメモリー・アレイ54に記憶される。情報は、メモリー・アレイ54のバンクの指定されたアドレス場所から読出され、出力マルチプレクサ53、出力バッファ52、データ・バス105aおよびバス102を介してホスト・プロセッサ5へ送られる。状態レジスタ58は、書込み状態マシンの状態、エラー中断状態、消去状態、プログラム状態およびVpp状態を記憶するために使用される。

【0062】書込み状態マシン61は、ブロックの消去を制御しかつプログラムのアルゴリズムを制御する。プログラム／消去電圧システム62は、Vppのレベルの関数として、メモリー・アレイ54のブロックまたは各ブロックのプログラミング・バイトの消去のため使用される（即ち、Vppがハイのレベルにある時、プログラミングが生じ得る；Vppがローのレベルならば、メモリー・アレイ54は読出し専用メモリーとして機能する）。

【0063】（動作の記述）本発明の機密保護メモリー・カードの動作については、特に図5、図6および図7のフロー図に関して以下に述べる。このような動作を詳

細に述べる前に、メモリー・カードの製造、特別調製および動作に含まれる諸ステップについて最初に述べることにする。

【0064】最初のステップとして、カードの製造時に、ACP10はメモリー・カード上の各メモリー・チップに対するロック値をセットする。ACP10は、キー値を図3および図4のロック・メモリーへロードすることによりこれを行う。これらの値は、ACPの保護不揮発性メモリー10-2（即ち、図2におけるキー1～n）に記憶される。次にロック記憶可能化論理要素36がゼロにセットされて、ロック・メモリーの内容のこれ以上の変更または読出しを禁止する。これら要素が不揮発性であるため、フラッシュ・メモリー・チップ全体がクリヤされなければ、変更することができない。

【0065】第2のステップとして、用途の特別調製時に、書込みが保護の機能により影響を受けないため、メモリー・カードはそのデータまたはソフトウェア・アプリケーションでロードすることができる。この時、ACP10はメモリーのバンク構造および各メモリー・バンクに与えられるべき保護の程度に関する情報でロードされる。

【0066】第3のステップとして、ユーザの特別調製時に、ユーザは確認データおよび要求される特定データの周期およびモードに対するパラメータ（例えば、個人識別番号（PIN））を確立する。

【0067】第4のステップとして、パワーオン時に、「キー・レジスタ」、「アクセス修正許容」信号および「アクセス制御メモリー」が初期設定されて、アクセス制御メモリー43に対するデータ・アクセスまたは書込みを禁止する。最初の確認対話が開始される。

【0068】最初の確認対話時に、ACP10は、そのホスト・プロセッサ5のサービスを用いてユーザを促して確認情報を受取る。確認が不成功であれば、動作は行われず、成功すれば、各々メモリー・チップのキー・レジスタがACPのメモリーに記憶された値でロードされる。この動作中、遅延カウンタ32が、成果のないプロセス乱打むな試みを行う以降のローディングの期間中チップの動作を禁止するため用いられるキー・レジスタのローディングは、「アクセス修正許容」信号を各チップにおいて真にさせる。その時、ACP10は、記憶された情報の構成に従ってアクセス制御メモリーをロードすることによりアクセスを確立する。

【0069】6番目のステップとして、以降の確認対話時に、ユーザの構成に従って、ACP10が別のユーザの確認（再確認）を促す。失敗の場合、ACP10は全てのメモリー・チップをそれらのパワーオン状態に強制し、これによりアクセス制御メモリー43をクリヤしかつキー・レジスタ31の内容をクリヤすることによりメモリーのデータに対するアクセスを禁止する。次に、図1のシステムの動作について図5、図6および図7に関

して記述する。

【0070】（遅延の最初の動作）図5および図6は、種々の動作モードをブロック図形態で示している。ブロック402および401は、2つの始動条件を示す。ブロック402において、ユーザはメモリー・カード3を前にパワーアップされたホスト・プロセッサ5に挿入する。ブロック401において、ユーザはホスト・プロセッサ5を既に組込んだメモリー・カード3でパワーアップする。

10 【0071】上記の始動動作のいずれかにおいて、ブロック402の間、ACP10およびそのインターフェースが従来周知の方法で初期設定され、ブロック403が「n」個のKレジスタ31と「n」個のアクセス制御メモリー43をフラッシュ・メモリー103a乃至103nの全てを内部初期設定シーケンスの一部としてクリヤする。これは、各メモリーにおける出力バッファ52が不能化されるため、メモリー103a乃至103nからデータが読出されることを阻止する。ロック値が、パワーオンの結果として各LM35から「n個の」Lレジスタ33にロードされる。

20 【0072】次にブロック404において、ACP10は、ユーザからPINまたは他の識別情報を要求することにより応答するホスト・プロセッサ5へ割込み信号を送る。ブロック405において、ACP10は、メモリー記憶域10-2aに記憶されたプログラムにより、前記PINまたは他の識別情報がメモリー記憶域10-2aに記憶された情報と一致することを調べる。もし一致しなければ、判断ブロック406がエラーをカウントして、ACP10がブロック404へ分岐してテストを反復する。テストが予め設定された回数失敗するならば、判断ブロック406はブロック407へ分岐してACP10をしてメモリー103a乃至103nの内容をロックアップあるいは破壊させる。

30 【0073】（成功した最初のユーザ確認）判断ブロック406において成功した確認を示す一致があるならば、ブロック408において、ACP10がロード・キー・レジスタ指令を介して、各Kレジスタ31を記憶場所10-2bから適当なキー値でロードする。また、ブロック409は遅延カウンタ32の内容を反復的に減分して、減分遅れカウンタ指令を2進数ゼロのカウントになるよう連続的に発行し、これが図3および図4におけるゼロ・カウント信号41の生成を生じる。

40 【0074】ブロック410において、アクセス制御メモリー43の各記憶域が読出し許容メモリー・バンク指令により情報がロードされて、対応するフラッシュ・メモリー103a乃至103nの選択されたバンクへのアクセスを許容する。

50 【0075】（間欠的な再確認）ブロック411において、ACP10は、ユーザの再確認を要求する前に、インターバル・カウンタ10-8により信号される記憶域

10-2に記憶された情報により確立される予め設定された時間間隔の終りを待機する。次いで、ブロック412において、ACP10は、ホスト・プロセッサ5に割込みをかけてユーザがPINまたは他の要求される識別を再入力することを要求する。

【0076】判断ブロック413は、ホスト・プロセッサ5から受取ったPINまたは他の情報を記憶域10-2aに記憶された情報に対して検査し、インターバル・カウンタ10-8出力が記録される。ユーザは、確認情報をホスト・プロセッサ5に入力する典型的に30秒の予め設定された時間間隔を有する。クロックが作動し続ける間、判断ブロック413のテストが失敗すると、ブロック414がこのテストをエラーとして記録する。この時、これは、最大数のエラーが受取られたかどうかを調べ、ブロック412および413を反復するため分岐する。エラー数が最大数と等しければ、ブロック415において、ACP10は連続的なロード・キー・レジスタ指令によりフラッシュ・メモリーのKレジスタ31をクリアし、連続的な読出し不能化メモリー指令によりアクセス制御メモリー43をクリアする。次にブロック415は、ブロック404へ分岐して新しい「最初の確認」動作が生じることを許容する。

【0077】判断ブロック413におけるテストが成功するならば、Kレジスタ31は変化しないままであり（即ち、ACPにより前にロードされたキー値を保持する）、ユーザがシステム1を動作させ続けることを可能にする。判断ブロック413がPINまたは他の情報を受取ることなく30秒が経過した場合、ACP10は前のようにKレジスタ31とアクセス制御メモリー43とをクリアする。

【0078】図7は、図5および図6のブロック404および412にตอบสนองして、ホスト・プロセッサ5がどのようにACP10からの割込み要求にตอบสนองするかを示すフロー図である。図示の如く、判断ブロック501は、ユーザがPINまたは他の情報を再入力することを要求するACP10からの割込みを待機する。判断ブロック501は、ブロック404または412から割込みを受取る時ブロック502へ分岐する。ブロック502は、ホストのディスプレイ5-2におけるPINまたは他の情報に対する要求を表示する。ブロック503は、キーボードからの情報を受入れ、ブロック504はACP10に割込みをかける。ブロック5はACP10に対してPINを送出する。

【0079】当業者には、本発明の教示から逸脱することなく本発明の望ましい実施態様に多くの変更が可能であることが判るであろう。例えば、本発明は、異なる形式の不揮発性メモリーおよび異なるインターフェースなどと共に用いることができる。

【0080】法規に従って本発明の最善の形態を記し示したが、頭書の特許請求の範囲に記載したように本発明

の趣旨から逸脱することなく変更が可能であり、ある場合には、本発明のある特徴を他の特徴に関わることなく有利に用いることができる。

【図面の簡単な説明】

【図1】本発明により構成されたメモリー・カードを組込んだシステムを示す全体ブロック図である。

【図2】不揮発性メモリーのレイアウトを含む図1のアクセス制御プロセッサ（ACP）を更に詳細に示すブロック図である。

10 【図3】本発明により修正された図1の標準的なフラッシュ・メモリーを示す更に詳細なブロック図である。

【図4】本発明により修正された図1の標準的なフラッシュ・メモリーを示す更に詳細なブロック図である。

【図5】種々の確認手順を実施する際の本発明のメモリー・カードの動作を説明するため用いられるフロー図である。

【図6】種々の確認手順を実施する際の本発明のメモリー・カードの動作を説明するため用いられるフロー図である。

20 【図7】種々の確認手順を実施する際の本発明のメモリー・カードの動作を説明するため用いられるフロー図である。

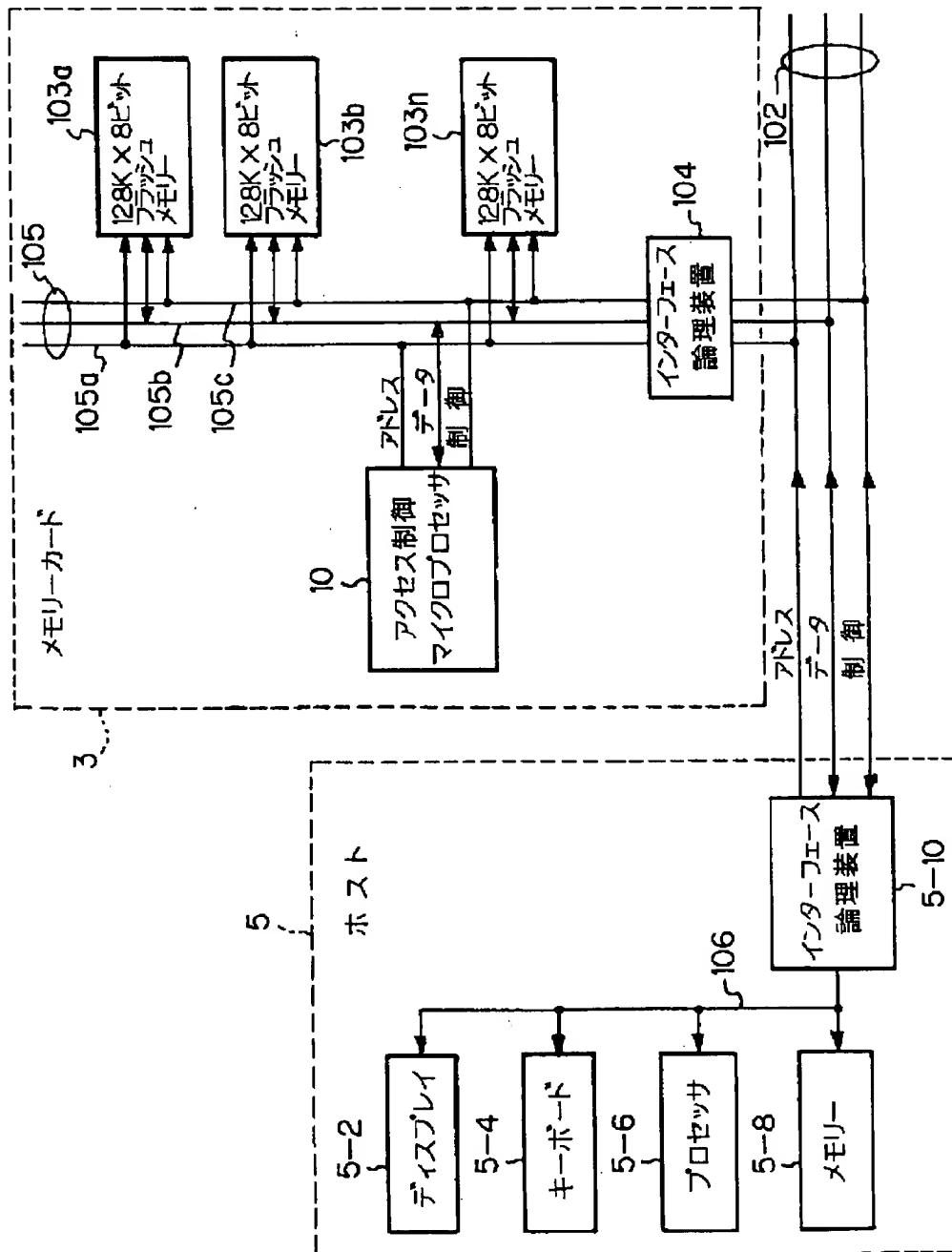
【符号の説明】

- 1 携帯可能な機密保護コンピュータ・システム
- 3 メモリー・カード
- 5 ホスト・プロセッサ
- 5-2 液晶ディスプレイ（LCD）
- 5-4 キーボード
- 5-6 マイクロプロセッサ
- 30 5-8 メモリー
- 5-10 直列インターフェース
- 10 アクセス制御プロセッサ（ACP）
- 10-2 保護不揮発性メモリー
- 10-4 ランダム・アクセス・メモリー（RAM）
- 10-6 マイクロプロセッサ
- 10-8 インターバル・カウンタ
- 10-10 インターフェース・ブロック
- 10-12 インターフェース論理装置
- 31 キー（K）・レジスタ
- 40 32 12ビット遅延カウンタ
- 33 32ビット揮発性ロック・レジスタ
- 34 アクセス修正許容ANDゲート
- 35 不揮発性ロック（L）・メモリー
- 36 1ビット不揮発性ロック記憶可能化要素
- 37 アクセス修正許容信号
- 38 全て1検出信号回路
- 39 コンパレータ論理回路
- 41 ゼロ・カウント信号
- 42 等価比較信号
- 50 43 揮発性アクセス制御メモリー

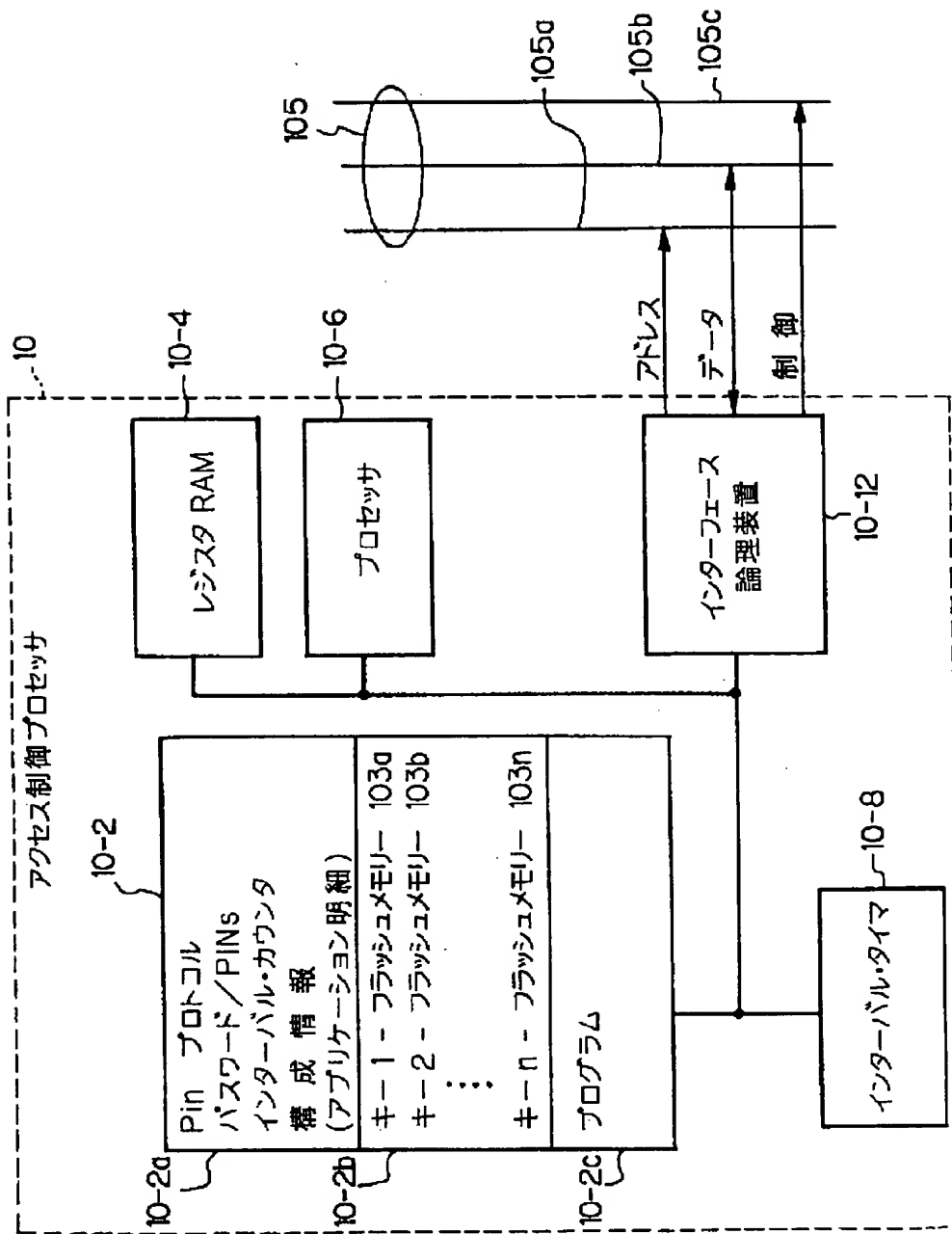
45 出力ORゲート
 50 指令レジスタ
 51 データ・レジスタ
 52 出力バッファ
 53 出力マルチプレクサ
 54 メモリー・アレイ
 56 アドレス・ラッチ
 58 状態レジスタ

* 60 入出力論理回路
 61 書込み状態マシン
 62 プログラム/消去電圧システム
 102 バス
 103a~n 128K×8ビットCMOSフラッシュ
 ・メモリー・チップ
 104 標準的インターフェース論理装置
 * 105 メモリー・カード・バス

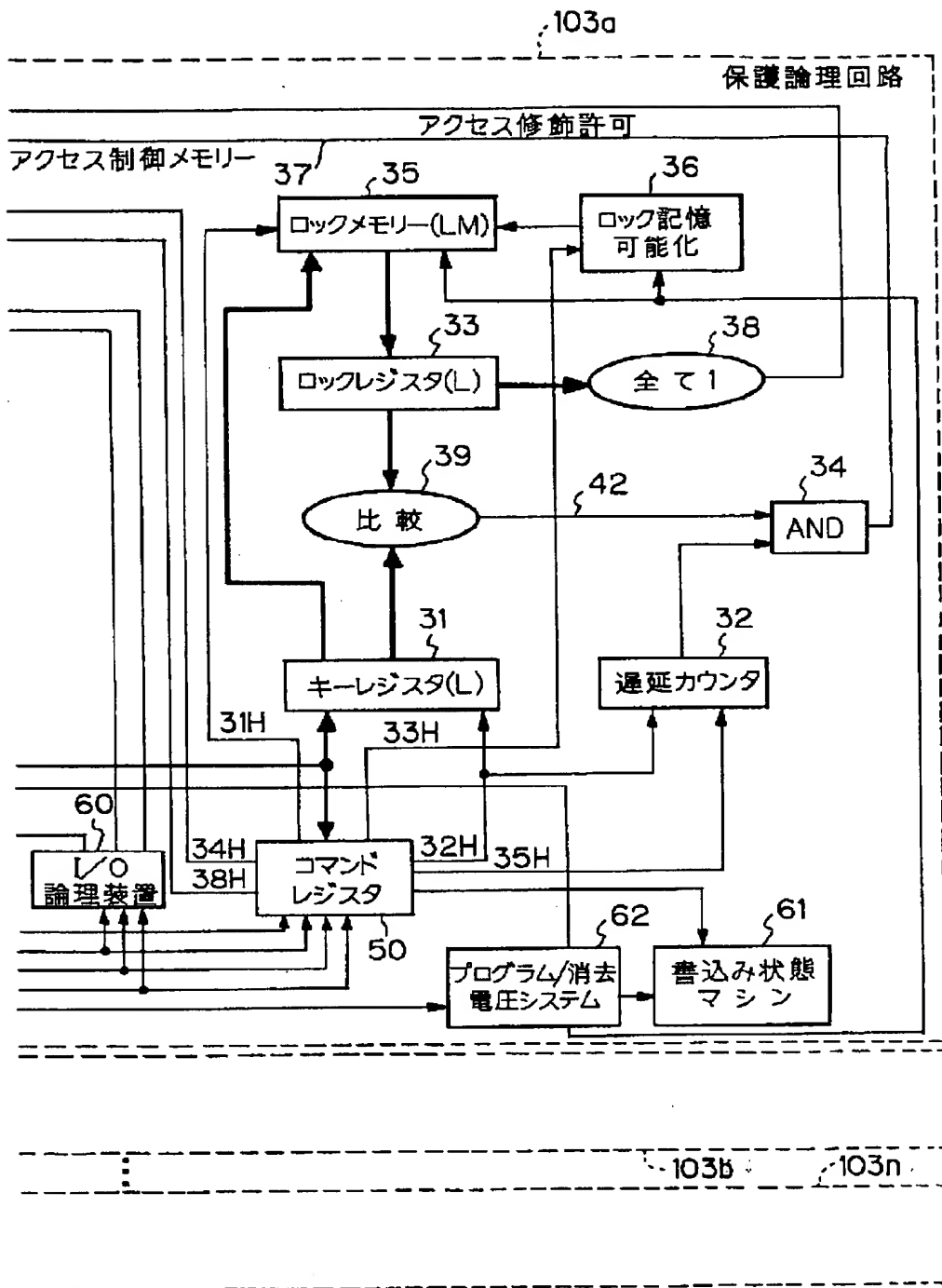
【図1】



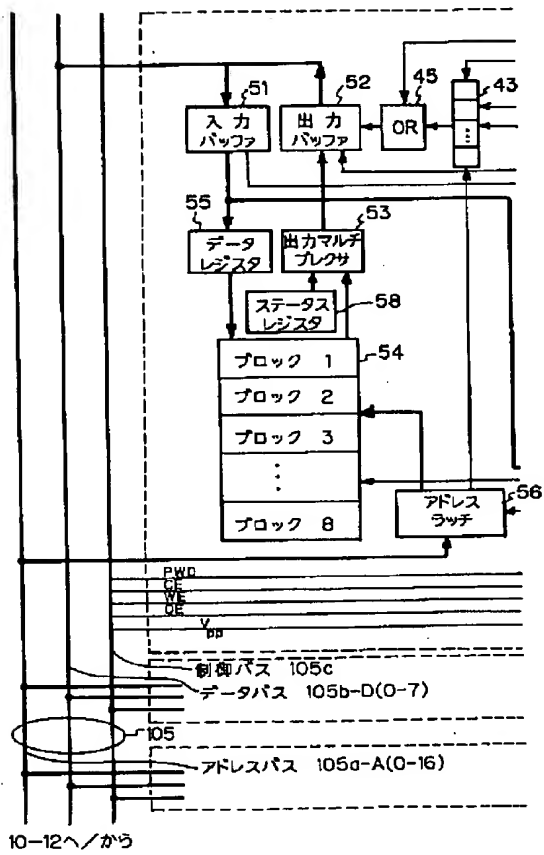
【図2】



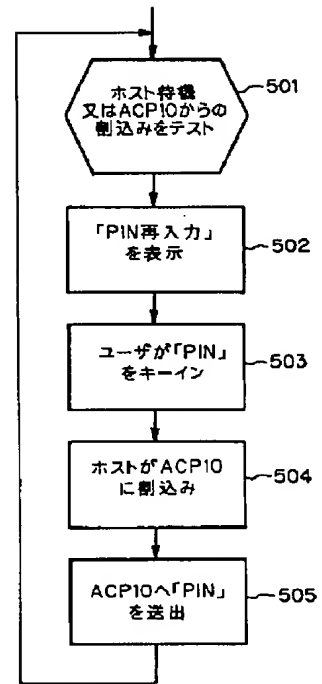
【図3】



【図4】

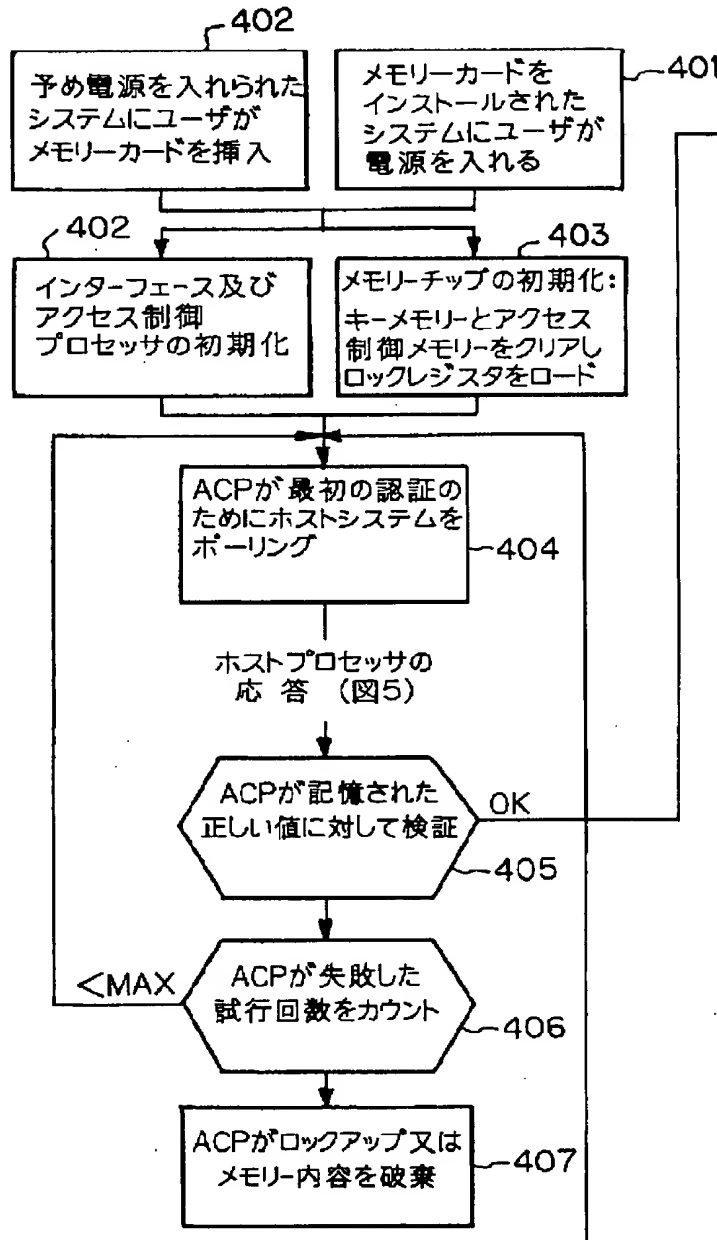


【圖 7】



【図5】

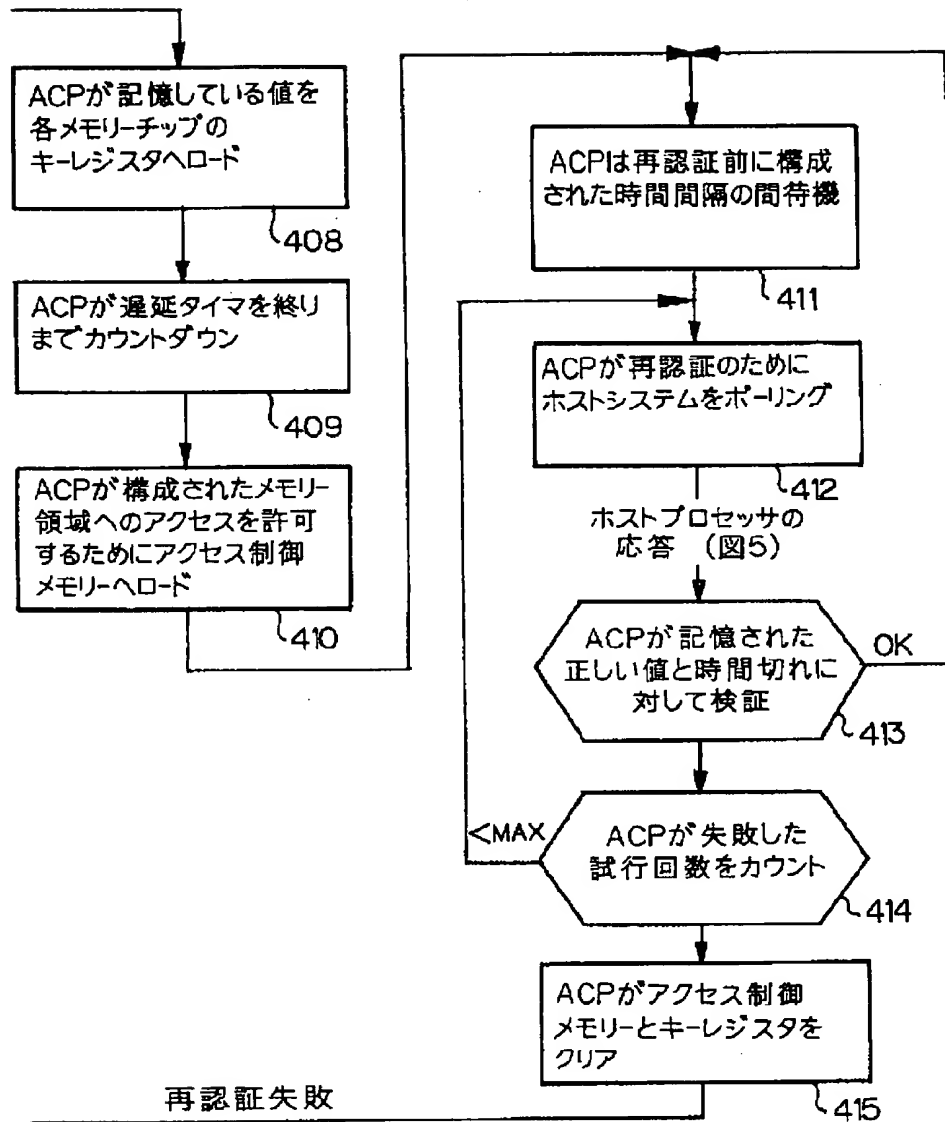
「1日の最初の操作」



【図6】

最初のユーザ認証成功

中間の再認証



フロントページの続き

(72)発明者 ビーター・ジェイ・ウィルソン
 アメリカ合衆国テキサス州78641 リーン
 ダー、フォレスト・トレイル 102

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第6部門第3区分
 【発行日】平成13年1月19日(2001. 1. 19)

【公開番号】特開平6-208515
 【公開日】平成6年7月26日(1994. 7. 26)
 【年通号数】公開特許公報6-2086
 【出願番号】特願平5-256786
 【国際特許分類第7版】
 G06F 12/14 320
 【F I】
 G06F 12/14 320 A

【手続補正書】

【提出日】平成11年6月29日(1999. 6. 29)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】ホストの携帯コンピュータと共に使用される機密保護メモリー・カードにおいて、前記ホスト・コンピュータに対しおよびこれからアドレス、データおよび制御情報を受受するように接続されたマイクロプロセッサを設け、該マイクロプロセッサは、複数のキー値を含む情報と構成情報とを記憶するアドレス指定可能不揮発性メモリーを含み、前記マイクロプロセッサに接続されて、アドレスとデータと前記カードにより行われるべきメモリー動作を定義する制御情報とを伝送する内部バスと、前記マイクロプロセッサと共通に前記内部バスに接続されて、前記アドレスとデータと制御情報とを受取る少なくとも1つの不揮発性のアドレス指定可能メモリーとを設け、前記メモリーは、不揮発性記憶セクションと機密保護制御セクションとを含み、該記憶セクションは複数のブロックに構成されたメモリー・アレイを含み、各ブロックは複数のアドレス指定可能な場所と前記記憶動作を行う制御論理手段とを有し、前記機密保護制御セクションは前記内部バスと前記制御論理手段と前記メモリー・アレイとに接続され、前記機密保護制御セクションは、前記ブロックと関連する少なくとも一つの前記キー値と構成情報を記憶する複数の不揮発性および揮発性記憶装置と、前記制御論理手段と前記記憶装置とに接続されたアクセス制御論理手段とを含み、該アクセス制御論理手段は、前記マイクロプロセッサが予め定めた確認手順が前記ホスト・コンピュータにより行われて前記アクセス制御論

理手段が前記構成情報に従って前記メモリー・アレイからの前記情報の読出しを許容することを可能にしたと判定した後のみ、前記構成情報により指定される如き前記メモリー・アレイの前記ブロックのアドレス指定されたものに記憶された情報の読出しを可能にすることを特徴とするメモリー・カード。

【請求項2】前記マイクロプロセッサおよび前記不揮発性メモリーが個々の半導体チップ上に含まれることを特徴とする請求項1記載のメモリー・カード。

【請求項3】前記カードが更に、該カードを前記ホスト・コンピュータに接続するインターフェース回路手段を含み、該インターフェース回路手段および前記マイクロプロセッサが同じ半導体チップ上に含まれることを特徴とする請求項1記載のメモリー・カード。

【請求項4】前記不揮発性メモリー・カードおよび前記不揮発性記憶装置がフラッシュ・メモリーであることを特徴とする請求項1記載のメモリー・カード。

【請求項5】前記不揮発性記憶装置の一方が、前記1つのキー値と対応するロック値を記憶するロック・メモリーであり、前記不揮発性装置の第2のものが前記ロック・メモリーに接続するロック記憶可能化要素であり、前記ロック・メモリーが最初に前記ロック値でロードされ、前記ロック記憶可能化要素が、前記マイクロプロセッサの制御下で前記ロック値の修正を禁止する状態へ切換えられることを特徴とする請求項1記載のメモリー・カード。

【請求項6】前記ロック値の記憶および前記ロック記憶可能化要素の切換えが、前記メモリー・カードの初期の製造中に起生することを特徴とする請求項2記載のメモリー・カード。

【請求項7】前記揮発性記憶装置の一方が、数において前記構成情報を記憶するための前記メモリー・アレイのブロック数と対応する複数の記憶域を持つアドレス指定可能なアクセス制御メモリーであり、該アクセス制御メモリーが前記内部バスと前記アクセス制御論理手段とに接続され、前記予め定めた確認手順が、前記アクセス

制御論理手段による前記アクセス制御メモリーの可能化を生じる前記ホスト・コンピュータにより最初に成功裏に行われたことを判定した後にのみ、前記アクセス制御メモリーが前記マイクロプロセッサの制御下でロードされることを特徴とする請求項5記載のメモリー・カード。

【請求項8】 前記ロック・メモリーにロードされた前記ロック値が全て1であり、前記機密保護制御セクションが更に、前記ロック・メモリーに接続された全て1の検出回路を含み、該検出回路が前記全て1のロック値にตอบสนองして、前記機密保護制御セクションを有効にバイパスする信号を生成して、前記不揮発性メモリーがあたかも前記機密保護制御セクションが含まれなかったかのように動作することを可能にすることを特徴とする請求項7記載のメモリー・カード。

【請求項9】 前記予め定めた確認手順の実施が、前記メモリー・カードが前記ホスト・コンピュータと通信するように最初に接続される時に初めて起生することを特徴とする請求項7記載のメモリー・カード。

【請求項10】 前記アクセス制御メモリーが、前記ロック・メモリーから前記ロック値を受取るように接続されたロック・レジスタと、コンパレータ回路と、前記マイクロプロセッサにより前記キー・レジスタに送られるキー値を記憶するキー・レジスタと、予め定めた時間間隔を定義するカウントを記憶する遅延カウンタと、前記アクセス制御メモリーと前記コンパレータと前記遅延カウンタとに接続されたゲート手段とを含み、前記コンパレータ回路が、前記ロックおよびキー・レジスタと前記ゲート手段とに接続され、該ゲート手段が前記遅延カウンタに接続されて、前記遅延カウンタが前記予め定めた時間間隔の終りを信号した時前記ロック・レジスタにロードされる前記ロック・コード値間の同じ比較を信号する前記コンパレータ回路にตอบสนองしてアクセス修正許可信号を生じ、前記アクセス修正許可信号が前記構成情報をロードするように前記アクセス制御メモリーを条件付ける信号を許可することを特徴とする請求項9記載のメモリー・カード。

【請求項11】 前記制御論理手段が、各メモリー・チップの前記機密保護制御セクションの動作を制御する際に前記マイクロプロセッサにより使用される予め定めた指令セットにตอบสนองして指令信号を生じる回路を含むことを特徴とする請求項10記載のメモリー・カード。

【請求項12】 前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの最初のものにตอบสนองして、前記ロック・コード値を前記ロック・メモリーにロードする第1の信号を生じ、該予め定めた指令の前記最初のものが前記カードの初期の製造中に生成されることを特徴とする請求項11記載のメモリー・カード。

【請求項13】 前記制御論理手段が、前記マイクロプロ

セッサにより生成された前記予め定めた指令セットの第2のものにตอบสนองして、前記ロック記憶可能化要素を、前記ロック・メモリーに記憶された前記ロック値に対する前記読出しまたは修正を禁止する予め定めた状態へ切換えるための第2の信号を生じることを特徴とする請求項12記載のメモリー・カード。

【請求項14】 前記制御論理手段が、前記マイクロプロセッサにより生じた前記予め定めた指令セットの第3のものにตอบสนองして、前記キー値の予め定めたもので前記予め定めたキー・レジスタをロードする第3の信号を生じ、前記予め定めた指令セットの前記第3のものが、前記予め定めた確認手順が成功裏に行われたことを前記マイクロプロセッサが判定した後にのみ、前記マイクロプロセッサにより生じることを特徴とする請求項12記載のメモリー・カード。

【請求項15】 前記制御論理手段により生じる前記第3の信号が、前記遅延カウンタを前記予め定めた時間間隔の開始を確立する予め定めたカウントに同時に強制し、前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの第4のものの各々にตอบสนองして前記予め定めたカウントを1だけ減分し、前記遅延カウンタが、前記予め定めた指令セットの予め定めた数の前記第4のものの実行に続く前記時間間隔の前記終りを信号することを特徴とする請求項14記載のメモリー・カード。

【請求項16】 前記予め定めた制御論理手段が、前記マイクロプロセッサによる前記予め定めた指令セットの第5および第6の複数にตอบสนองして、情報の読出しが許容される前記ブロックのどれかを判定するため前記構成情報に従って前記アクセス制御メモリーにおける場所をセットしリセットするための第5および第6の信号を生じることを特徴とする請求項11記載のメモリー・カード。

【請求項17】 前記ホスト・コンピュータとの通信を確立するためホストの携帯コンピュータに組込み可能な機密保護メモリー・カードにおいて、単一の半導体チップ上に含まれるマイクロプロセッサを設け、該マイクロプロセッサは、前記ホスト・コンピュータに対しかつこれからアドレスとデータと制御情報とを送受するよう接続され、該マイクロプロセッサは、記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するメモリー読出しアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、アドレスとデータと前記カードにより行われるべき記憶動作を定義する制御情報とを送受する内部バスと、前記アドレスとデータと制御情報とを受取るため前記マイクロプロセッサと共通に前記内部バスに接続された少なくとも1つの不揮発性のアドレス指定可能なメモリー

・チップとを設け、該メモリー・チップは1つの記憶セクションと1つの機密保護セクションとを含み、該記憶セクションはデータ出力を有する不揮発性のメモリー・アレイを含んで各々が複数のアドレス指定可能な場所を有する複数のブロックに構成され、前記記憶動作を行うための制御論理手段を含み、前記機密保護セクションは、前記内部バスと前記制御論理手段と前記データ出力とに接続され、該機密保護セクションは、前記内部バスに接続されて前記キー値数の1つと合致する予め定めたロック値を最初に受取りかつこれを恒久的に記憶する不揮発性ロック・メモリーと、前記制御論理手段および前記ロック・メモリーと接続されて、前記予め定めたロック・コード値が前記マイクロプロセッサにより前記内部バスに与えられた前記キー値の選択された1つに識別可能に合致する時を検出すると同時に、可能化信号を生じるアクセス制御論理手段と、前記読出し可能性を定義する前記記憶構成情報を記憶するための数において前記メモリー・アレイの前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、前記アクセス制御メモリーが、前記制御論理手段と前記メモリー・アレイのデータ出力と前記内部バスと前記アクセス制御論理手段とに接続され、該アクセス制御論理手段は、予め定めた確認手順が前記ホスト・コンピュータにより成功裏に行われ、かつ前記記憶のキー・コードの前記予め定めた1つを転送して、前記アクセス制御メモリーの構成情報により指定される如き前記データ出力に加えるための前記可能化信号を、前記アクセス制御論理手段をして前記データ出力に加えられる前記可能化信号を生じさせたことを前記マイクロプロセッサが判定した後にのみ、前記記憶構成情報により指定される如き前記メモリー・アレイの読出しを可能にすることを特徴とするメモリー・カード。

【請求項18】 各々が複数のモードにおける動作能力を有するアドレス指定可能な場所のブロックに構成されたメモリー・アレイを含む複数の不揮発性メモリー・チップを含む機密保護メモリー・カードにおいて、ロック値を記憶するロック・メモリーと、第1および第2の指令と予め定めたキー値とを生成する制御手段と、前記制御手段に接続されて、前記第1の指令にตอบสนองして前記予め定めたキー値を記憶するキー・レジスタと、前記ロック・メモリーおよび前記キー・レジスタに接続され、前記ロック値および前記予め定めたキー値が等しい時は常に比較信号を生成するコンパレータと、前記生成手段に接続され、かつ前記第1の指令にตอบสนองして前記カウンタを最大カウント値に設定し、かつ一連の連続する第2の指令にตอบสนองして前記遅延カウンタがゼロに減分された時ゼロ・カウント信号を生じる遅延カウンタと、

前記コンパレータおよび前記遅延カウンタに接続され、前記比較信号および前記ゼロ・カウント信号にตอบสนองしてアクセス修正許容信号を生じる論理回路手段とを設け、前記制御手段が、第3の指令と、前記第1のブロックおよび以降のブロックをそれぞれ識別する第1のアドレス信号と以降のアドレス信号とを生じ、前記論理手段と前記制御手段とに接続されたアクセス制御メモリー手段を設け、該アクセス制御メモリーは、前記アクセス記憶可能化信号と前記アドレス信号と前記第3の指令とにตอบสนองして、前記ブロックおよび前記以降のブロックの内の一つが読出しのため可能状態にされる時を指定する表示を記憶することを特徴とするメモリー・カード。

【請求項19】 前記メモリー・カードが不当なホスト・コンピュータに配置される時、前記予め定めた値および最大値が、前記不揮発性メモリーに記憶された前記情報に対する容易なアクセスを阻止するように充分に大きく選定されることを特徴とする請求項18記載のシステム。

【請求項20】 前記制御手段が、第1のユーザの確認動作を成功裏に行ったと同時に、前記第1、第2および第3の指令を生じる前記メモリーに接続するマイクロプロセッサを含むことを特徴とする請求項18記載のカード。

【請求項21】 前記第1の指令がロード・キー指令であり、前記第2の指令が減分指令であり、前記第3の指令が読出し許容ブロック指令であることを特徴とする請求項20記載のカード。

【請求項22】 前記メモリーが更に、前記カードを正常な記憶動作を行うように条件付ける予め定めた指令セットを復号する指令制御手段を含み、前記指令制御手段が、前記第1、第2および第3の指令を含む別の指令セットを復号して前記メモリーに記憶された情報に対する機密保護を行う手段を含むことを特徴とする請求項18記載のカード。

【請求項23】 各々がアドレス指定可能な場所に構成されたメモリー・アレイを含む複数の不揮発性メモリー・チップと、記憶動作を行う指令信号を生じる制御論理回路を含むホスト・コンピュータに組込み可能な機密保護メモリー・カードを構成する方法において、

(a) 組込まれた時前記ホスト・コンピュータと通信するように接続される前記カードにマイクロプロセッサを組込み、該マイクロプロセッサは、記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、

(b) 機密保護論理回路を各不揮発性メモリー・チップに組込み、該機密保護論理回路が、予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メ

モリーと接続されたアクセス制御論理手段と、前記構成情報に従ってアクセス可能性のビット情報を記憶する前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリとを含み、

(c) 前記マイクロプロセッサを各メモリ・チップに組込み、アドレスとデータと制御情報とを前記各メモリ・チップへ転送し、

(d) 複数の指令にตอบสนองして前記機密保護論理回路を動作させるよう前記制御論理回路を修正し、

(e) 前記ホスト・コンピュータと共に前記マイクロプロセッサによる初期の予め確立されたユーザ確認動作を実施し、

(f) ステップ(e)における前記確認動作が成功裏に行われた時にのみ、前記各チップに対して前記複数の指令の特定のものを転送する前記マイクロプロセッサにより前記機密保護論理回路を可能状態にして、前記ブロックの異なるものに記憶された前記情報を前記アクセス制御メモリに記憶された前記アクセス可能性ビット情報に従って読出すことを許容するステップを含むことを特徴とする方法。

【請求項24】 前記マイクロプロセッサの不揮発性メモリが複数のセクションを有し、ステップ(a)が更に、前記キー値に対する乱数を生成して該キー値を前記セクション数の最初のものにロードするステップを含むことを特徴とする請求項23記載の方法。

【請求項25】 前記マイクロプロセッサが更に、前記マイクロプロセッサの不揮発性メモリに接続されたインターバル・カウンタを含み、ステップ(a)が更に、ユーザが選択した時間間隔を生成して該ユーザ選択時間間隔値と対応する値を前記インターバル・カウンタへロードするステップを含み、更に

(g) 前記ユーザ選択時間間隔でステップ(e)の前記ユーザ確認動作を周期的に開始し、

(h) ステップ(b)の前記確認動作が成功裏に行われる限り、前記ブロックに記憶された前記情報が前記アクセス可能性ビット情報に従って読出されることを許容し続けるステップを含むことを特徴とする請求項24記載の方法。

【請求項26】 各々がアドレス指定可能な場所のブロックに構成されたメモリ・アレイを含む多数の情報を記憶するための複数の不揮発性メモリ・チップと、記憶動作を行うための指令信号を生成する制御論理回路とを含む機密保護メモリ・カードを構成する方法において、

(a) 記憶域に対するユーザのアクセス可能性を定義する多数のキー値を含む情報と、前記記憶域に対するアク

セス可能性を定義するメモリ構成情報とを記憶するためのアドレス指定可能な不揮発性メモリを含むマイクロプロセッサを前記カードに組込み、

(b) 予め定めたロック値を記憶する不揮発性ロック・メモリと、該ロック・メモリに接続されたアクセス制御論理手段と、前記構成情報に従ってユーザのアクセス可能性ビット情報を記憶する前記多数のブロックと数において対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリとを含む機密保護論理回路を各不揮発性メモリ・チップに組込み、

(c) アドレスとデータと制御情報とを前記各メモリ・チップへ転送するため前記マイクロプロセッサを各メモリ・チップに相互に接続し、

(d) 前記制御論理回路により通常与えられる1組の指令に対する拡張として前記機密保護論理回路を動作させる複数の指令を組込むように前記制御論理回路を修正することにより、前記機密保護論理回路が、前記多数のチップが前記メモリ・カードから取外される場合でも、前記チップに含まれる前記情報が不当な方法で読出されることを防護するステップを含むことを特徴とする方法。

【請求項27】 不揮発性記憶セクションと機密保護制御セクションとを含む不揮発性メモリ・チップ(103a)であって、前記記憶セクションは、一方では、夫々複数のアドレス指定可能な場所を有する幾つかのブロックに構成されたメモリ・アレイ(54)を、他方では、記憶動作を行う制御論理手段(50)を含み、前記機密保護制御セクションは、前記制御論理手段及び前記メモリ・アレイに接続されており、該機密保護制御セクションが、
前記ブロックと関連する少なくとも1つのキー値と構成情報を記憶する複数の不揮発性記憶装置(31、35)及び揮発性記憶装置(33、43)と、
前記制御論理手段(50)と前記複数の記憶装置に接続されたアクセス制御論理手段(32、34、39)とを含み、該アクセス制御論理手段は、前記メモリ・チップ(103a)が外部のマイクロプロセッサ(10)から予め定めた認証手順がユーザによって実行されたことを示す信号を受け取った後にのみ、前記構成情報によって特定された前記メモリ・アレイ(54)のアドレス指定された前記ブロックの内の1つに記憶された情報の読み出しを可能にし、前記アクセス制御論理手段(32、34、39)が前記構成情報に従って前記メモリ・アレイ(54)から前記情報の読み出しを許すことを可能にする、
ことを特徴とするメモリ・チップ。